AF
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Applicant : Barry Lynn Royer

Serial No. : 09/817,323

Filed : March 26, 2001

For : A SYSTEM AND USER INTERFACE FOR ADAPTIVELY PROCESSING AND COMMUNICATING URL DATA BETWEEN APPLICATIONS

Examiner : Zachary A. Davis

Art Unit : 2137

APPEAL BRIEF

May It Please The Honorable Board:

This is Appellants' Brief on Appeal from the final rejection of claims 1 – 20. Please charge the $500.00 fee for filing this Brief to Deposit Account No. 19-2179. Appellants waive an Oral Hearing for this appeal. Enclosed is a single copy of this brief.

Please charge any additional fee or credit overpayment to the above-indicated Deposit Account. Enclosed is a single copy of the Brief.

Appellants do not request an oral hearing.

****

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in a postage paid envelope addressed to: Mail Stop: Appeal Briefs - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Signature Alexander Burke Date: 6 September 2005

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 09/817,323 is the Assignee of record:

Siemens Medical Solutions Health Services Corporation
51 Valley Stream Parkway
Malvern, PA 19355-1406

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no related Appeals or Interferences regarding Application Serial No. 09/817,323.

III. STATUS OF THE CLAIMS

Claims 1 24 are rejected and the rejection of claims 1-24 are appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the claims included in Appendix I.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 describes a system employed by a first application for encoding URL link data for use in detecting unauthorized URL modification (page 1, para. 4). An input processor receives an encryption key and a URL processor adaptively processes a URL link to a second application differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link (page 2, para. 1-3). A communication processor includes the processed URL in data representing a web page and communicates

the web page representative data including the processed URL to a requesting application (page 2, para. 3).

Dependent claim 2 includes all the limitations contained in independent claim 1 and further provides that the encryption key is accessible by the first and second applications from a managing application (page 7, para. 1; Figure 5, 530).

Dependent claim 3 includes all the limitations contained in independent claim 1 and further provides that the communication processor communicates the URL link address portion to a managing application for encryption (page 5, para. 2).

Dependent claim 4 includes all the limitations contained in independent claim 1 and further provides that the URL processor of the first application adaptively processes the URL link to the second application differently to the link to the web page provided by the first application in response to an identified URL type (page 2, para. 1).

Dependent claim 5 includes all the limitations contained in dependent claim 4 and further provides that the URL link to the second application includes an encrypted address portion and the link to the web page provided by the first application includes non-encrypted address portion (page 13. para. 1).

Dependent claim 7 includes all the limitations contained in independent claim 1 and further provides that the URL processor compresses the URL link address portion and encrypts a compressed URL link address portion (page 11, para. 3).

Dependent claim 8 includes all the limitations contained in dependent claim 7 and further provides that the URL processor compresses the URL link address portion using a hash function (page 11, para. 3).

Dependent claim 9 includes all the limitations contained in dependent claim 7 and further provides that the communication processor communicates the URL link address portion to a managing application for compression (page 11, para. 3).

Dependent claim 10 includes all the limitations contained in independent claim 1 and further provides that the URL processor adaptively generates URL fields including encrypted patient specific information for incorporation in the URL link to the second application (page 2, para. 3).

Independent claim 11 recites a system for encoding URL link data for use in detecting unauthorized URL modification occurring during concurrent operation of a plurality of applications. The system comprises a managing application for providing a common encryption key to a plurality of concurrently operating applications. The first application includes an input processor for receiving the encryption key and a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link. The first application further includes a communication processor for including the processed URL in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application (page 1, para. 4).

Dependent claim 12 includes all the limitations contained in independent claim 11 and further provides that the communication processor communicates the URL link address portion to the managing application for encryption (page 5, para. 2).

Dependent claim 13 includes all the limitations contained in independent claim 11 and further provides that the URL processor compresses the URL link address portion and encrypts a compressed URL link address portion (page 2, para. 1).

Dependent claim 14 includes all the limitations contained in dependent claim 13 and further provides that the URL processor compresses the URL link address portion using a hash function (page 5, para. 3).

Dependent claim 15 includes all the limitations contained in dependent claim 13 and further provides that the communication processor communicates the URL link address portion to the managing application for compression (page 11, para. 3).

Independent claim 16 recites a system for encoding URL link data for use in detecting unauthorized URL modification. The system includes a browser application for providing a user interface display permitting user entry of identification information for providing user identification information to a first application. The first application is responsive to the user identification information including a URL processor for adaptively generating URL fields including an encrypted URL address portion and encrypted patient specific information for incorporation together with a non-encrypted portion in a processed URL. A communication processor is used for including the processed URL in data

representing a web page and for communicating the web page representative data including the processed URL to a requesting application.

Dependent claim 17 includes all the limitations contained in independent claim 16 and further provides that the communication processor communicates the URL address portion and the encrypted patient specific information to another application for encryption.

Independent claim 18 recites a system for processing URL link data for detecting unauthorized URL modification and suitable for use by a plurality of concurrently operating applications. The system comprises a first application including a URL processor for adaptively generating a URL link to a second application differently to a URL link to a web page provided by the first application, to provide a generated URL by using a received encryption key to encrypt a URL link address portion of the URL link to the second application and by non-encryption of the URL link to the web page provided by the first application. The first application further includes a communication processor for including the generated URL in data representing a web page and for communicating the web page representative data including the generated URL to a requesting application.

Dependent claim 19 includes all the limitations contained in dependent claim 18 and further provides that the URL processor generates a URL field including encrypted patient specific information for incorporation in the generated URL link to the second application.

Independent claim 20 recites a system supporting concurrent operation of a plurality of Internet compatible applications. The system comprises a browser application including a display generator for providing a user interface display permitting user entry of

identification information and commands for a plurality of Internet compatible applications and for providing user identification information to a first application. The system further comprises a URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a non-encrypted session identifier. The system also comprises a processor for initiating communication of the generated URL to the first application in response to validation of the user identification information, the first application having access to a key for decrypting the encrypted URL address portion (page 13, para. 1).

Independent claim 21 recites a method for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. An encryption key is received and a URL link to a second application is processed using the received encryption key by identifying URL type and adaptively encrypting a URL link address portion based on the identified type to produce a processed URL. The processed URL is included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application (page 12, para. 3).

Independent claim 22 recites a method employed by a first application operating in a system supporting concurrent operation of a plurality of Internet compatible applications. In response to a command from a request device to initiate a first application, user operability of the first application is enabled based upon validation of user identification information. A link to a second application is encrypted. The encrypted link in data representing a web page is included to be returned to the request device. The web page representative data including the encrypted link is communicated to the request device (page 6, para. 3).

Independent claim 23 recites a method for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. A common encryption key is provided to the plurality of concurrently operating applications and encryption key is received. A URL link to a second application using the received encryption key is processed by identifying URL type and adaptively encrypting a URL link address portion based on the identified type to produce a processed URL. The processed URL is included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application (page 12, para. 3).

Independent claim 24 recites a method for processing URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. A URL link to a second application is adaptively generated differently to a URL link to a web page provided by the first application to provide a generated URL. The generated URL is included in data representing a web page and for communicating the web page representative data including the generated URL to a requesting application (page 12, para. 3).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner has rejected claims 1-9, 11-15, 18, 20, 21, 23 and 24 as being anticipated under 35 USC 102(b) by Levergood et al. (US 5,708,780).

The Examiner has rejected claims 10, 16, 17 , 19 and 22 as being unpatentable under 35 USC 103(a) over Levergood et al. in view of Berman et al (US 5,995,939).

VII. ARGUMENT

Levergood et al. when taken alone or in combination with Berman et al. neither anticipate nor make unpatentable the present claimed invention. Thus, reversal of the Final Rejection (hereinafter termed "rejection") of claims 1-24 under 35 U.S.C. §§ 102(b) and 103(a) is respectfully requested.

Overview of the Cited References

Levergood et al. describe a method for controlling and monitoring access to network servers. In particular, the process described in the invention includes client-server sessions over the Internet involving hypertext files. In the hypertext environment, a client views a document transmitted by a content server with a standard program known as the browser. Each hypertext document or page contains links to other hypertext pages which the user may select to traverse. When the user selects a link that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain.(See Levergood et al., Abstract)

Berman et al. disclose an automated networked service request and fulfillment system including client computer systems in the offices of professionals such as doctors, and sponsor computers at the sites of service providers such as test labs or insurance companies, interconnected with a mail server system that exchanges e-mail messages via the Internet or a similar network. Service requests, such as ordering a medical test or requesting authorization for a particular procedure, are prepared using a client system and automatically e-mailed to the sponsor system of an appropriate service provider. The

request is fulfilled and the results e-mailed back to the requesting client system using the mail server system. Confidentiality is insured by encrypting all e-mail messages. The system includes a universal interface component which automates the process of converting data records found in existing databases into the data record format required by the new system. (See Berman et al.; Abstract)

Rejection of Claims 1-9, 11-15, 18, 20, 21, 23 and 24 under 35 USC 102(b) over Levergood et al. (US Patent No. 5,708,780).

Reversal of the rejection of claims 1-9, 11-15, 18, 20, 21, 23 and 24 under 35 U.S.C. 102(b) as being unpatentable over Levergood et al. is respectfully requested. The rejection erroneously states that claims 1-9, 11-15, 18, 20, 21, 23 and 24 are anticipated by Levergood et al. for the reasons discussed herein below.

CLAIMS 1 and 6

The Office Action suggests that Levergood et al. disclose a system including an input processor that receives an encryption key (column 5, lines 61-65), a URL processor that adaptively processes a URL link to a second application by encrypting a URL address portion (column 5, line 61-65; column 3, lines 34-37; and column 4, line 1-18) and by not further encrypting a link within the first application (column 3, lines 56-67), and a communication processor that includes the processed URL in web page data (column 6, lines 17-26). Applicant respectfully disagrees.

Rather, Levergood et al. describe an internet server access control and monitoring system. When a user selects a link that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an

authorization or valid account. Upon verification, the user is provided with a session identification, allowing the user to access the requested file as well as any other files within the present protection domain.

In contrast, Claim 1 of the present invention recites a system "employed by a first application for encoding URL link data for use in detecting unauthorized URL modification" comprising "an input processor for receiving an encryption key; a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link; and a communication processor for including the processed URL in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application".

Specifically, the system of claim 1 involves "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". This is done "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". These features address the security deficiencies of URL processing functions of electronic systems, such as those described in Levergood et al. As stated on page 11, lines 1-9 of the present specification, "Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause

URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted."

The claimed system addresses the security problem that is present in prior art systems such as Levergood et al. by "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 1 of the present invention. However, the user selection of the embedded link to view laboratory test orders in browser command does not require the incorporation of the session identifier and other context information, as stated in the present specification on page 14, lines 34-36, "because the link to the test results page is an intra-application link there is no requirement for this particular embedded link to be processed in the manner previously described to incorporate the session identifier and other context information".

Levergood et al. neither disclose nor suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application" as in the present invention. Levergood et al. also fail to show or suggest doing this "by using said received encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". In an exemplary embodiment of the invention illustrated in the Application specification pages 11-12, application 200 advantageously, for example, encrypts "a **URL** link **address portion**" comprising a hash value identified by

field identifier GSH= derived by "hashing on the **addressable portion** of a fully qualified URL" **comprising** the "URL data either lying between the "http://" and the question mark "?" or from the data lying between the "http://" and the pound/number sign "#" - whichever comes first" (Application page 10 lines 1-2 and page 11 line 27). Consequently, in the exemplary URL string shown processed in the specification page 12

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937&GSH=24017&Pid=1772693&Frgclr=blue

the compressed address portion is 24017 which is concatenated with a patient identifier (specification page 12 line lines 17-21) as shown:

GSH=24017&Pid=1772693

and is encrypted into the string

16sfdjwhejeyw7rh3hekw

to produce the processed URL including the encrypted URL address portion:

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937:16sfdjwhejeyw7rh3hekw&Frgclr=blue.

This is an exemplary "processed URL". Therefore, Applicant respectfully submits that the Rejection makes a **fundamental error** on page 3 in interpreting the Levergood et al. reference. Contrary to the Rejection statements on page 3, Levergood et al. in column 5

lines 61-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers"- (Levergood et al. column 5 lines 61-65, also see column 3 lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link." The claimed "address portion" is NOT (and is NOT suggested by) the "SID" or "IP address" of Levergood.

Further, although in Levergood et al. a valid session identifier "typically comprises" an "accessible domain" in the "SID encrypted with a secret key", the Levergood et al. accessible domain is NOT a URL or an address portion of a URL (Levergood et al. column 3 lines 33-37). Levergood et al. explicitly define an accessible "domain" as a collection of files and NOT a URL or address portion of a URL ("A protection domain is **defined** by the service provider and is a **collection of controlled files** of common protection within one or more servers" – Levergood et al. column 3 lines 52-55). This is further made clear in column 5 lines 54-61 stating a "preferred SID is a sixteen character ASCII string that encodes **96** bits of SID data" that contains "an **8**-bit **domain** comprising **a set of information files** to which the current SID authorizes access". Such an "accessible domain" as used by Levergood et al. is not in a URL link address portion. This is further corroborated in Levergood et al. in column 6 lines 29-34 indicating that such a domain is in the **non-address**, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?**domain=** [domain]& URL = http://content.com/report".

The Examiner states in his Advisory Action that if the domain includes a collection of files within a server, then the "domain must include an identification and/or address for these files", thus the domain can indeed include an address portion of a URL. However, nowhere in Levergood et al. is it disclosed or suggested that the domain includes a URL or even a portion of a URL. In fact, Levergood et al. explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. The Examiner's reliance on interpreting "a collection of files" to anticipate "using a received encryption key to encrypt a URL link address portion" is a **fundamental error.** In so doing, the Examiner is not only engaging in the pure speculation that the Levergood "collection of files" has something to do with a URL, but also that it leads to teaching encryption of a "URL address portion" as specifically defined in the present Application. Further, this speculation is without foundation and **directly contradicts** Levergood's own teaching in column 5 line 59 that a domain is an 8 – bit value ("SID data" contains "an **8**-bit **domain** comprising **a set of information files"**). Thus, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention.

Levergood et al. do not show or suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL". Neither a session identifier nor an IP address as used in Levergood et al. are a "URL or a URL address portion" as in the present claimed invention. Specifically, a URL and IP address are distinct and different objects with totally different functions. This is evidenced in column 5, lines 37-38 of Levergood et al. which states that "the content server records the URL **and** the IP address." An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host

name of the machine that holds the file, and the **path** to the file" (Levergood et al. column 2 lines 28-31). On the other hand, a session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11 line 19). Thus, neither a session IP nor an IP address is equivalent to "a URL link address portion of said URL link" as in the present claimed invention.

Levergood et al. also neither disclose nor suggest the claim 1 feature combination involving "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). In contrast, the present claimed invention addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9).

Levergood et al. further neither disclose nor suggest the claim 1 feature of "for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application ". While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention.

Thus Levergood et al. do not anticipate claim 1 of the present invention. Claim 6 is also considered patentable based on its dependence on claim 1. Consequently, as the Levergood et al. system neither disclose nor suggest each element of the claimed

arrangement, Levergood et al. do not anticipate the invention claimed in claim 1 and 6. Therefore, withdrawal of the rejection of claims 1 and 6 under 35 USC 102(b) is respectfully requested.

CLAIM 2

Dependent claim 2 is considered to be patentable based on its dependence on claim 1. Claim 2 is also considered to be patentable because Levergood et al. neither disclose nor suggest the use of an "encryption key...accessible by said first and second applications from a managing application". Levergood et al. disclose that an encryption key used for encrypting an IP address (NOT a URL address portion) is accessible by a content and authorization server (Levergood et al. column 5 lines 61-65) but fails to show or suggest an encryption key for encrypting a "URL address portion" is accessible from a "managing application" by different "first and second applications". It is contended in the Advisory Action that an IP address portion is the same as a URL address portion for the same reason that a domain can include an address portion of a URL. However, nowhere in Levergood et al. is it disclosed or suggested that an IP address includes a URL or even a portion of a URL. Again the Examiner appears to directly contradict the Levergood reference. A URL and IP address are distinct and different objects with totally different functions. This is evidenced in column 5, lines 37-38 of Levergood et al. which states that "the content server records the URL **and** the IP address." An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" (Levergood et al. column 2 lines 28-31). Consequently, as the object encrypted by Levergood et al. (IP address) is not equivalent to the object encrypted in the present claimed invention ("a URL address portion of a URL"), Levergood et al. neither disclose nor suggest that the "encryption key is accessible by said first and second applications from a managing application" as recited in

claim 2 of the present invention. Thus, Levergood et al. do not anticipate claim 2 of the present claimed invention.

CLAIM 3

Dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Levergood et al. do not show (or suggest) the "communication processor communicates said URL link address portion to a managing application for encryption". The Examiner notes that in Levergood et al., the authentication server generates the session identifier which includes performing encryption. Levergood et al. do not suggest such a separate managing application used for encryption of URL data and operating in conjunction with distinct "first and "second" applications. Instead, Levergood et al., in column 5, lines 44-49 relied on in the Rejection merely mentions redirecting a URL to an authentication server for authenticating a **session identifier**. This is not "communicat[ing] said URL link address portion to a managing application for encryption" as in the present claimed invention.

It is further asserted in the Advisory Action that Levergood et al. discloses the session identifier includes the domain, and if the domain includes a collection of files within a server, then the domain must include an identification and/or address for these file, thus the domain can indeed include an address portion of a URL. However, nowhere in Levergood et al. is it disclosed or suggested that the domain includes a URL or even a portion of a URL. In fact, Levergood et al. explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. Thus, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention. Consequently, Levergood et al. does not anticipate claim 3 of the present claimed invention.

CLAIM 4

Dependent claim 4 is considered to be patentable based on its dependence on claim 1. Claim 4 is also considered to be patentable because Levergood et al. neither disclose nor suggest that the "URL processor of said first application adaptively processes said URL link to said second application differently to said link to said web page provided by said first application in response to an identified URL type" as in the present claimed invention. Levergood et al., contrary to the Rejection statement on page 4 of the Office Action, do not show any form of adaptive URL processing in response to "URL type" or even mention or suggest "URL type" in column 3, line 56 to column 4, line 24, or elsewhere. The Examiner contends that a "relative link" and an "absolute link" can define types of URL links. However, nowhere in Levergood et al. is it disclosed or suggested that the relative or absolute link defines a type of URL link. In fact, the relative link, as discussed column 3, lines 60-61 of Levergood et al., may be made either within the same domain or to a different domain. As stated above in regards to claim 1, Levergood et al. neither disclose nor suggest that the domain includes a URL or even a portion of a URL. In fact, Levergood et al. explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. Thus, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention. Consequently, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention. Because Levergood et al. does not discriminate between URL types, Levergood et al. can not "adaptively process" links "in response to an identified URL type" as in the present invention. Thus, Levergood et al. do not anticipate claim 4 of the present claimed invention.

CLAIM 5

Dependent claim 5 is considered to be patentable based on its dependence on claims 1 and 4. Claim 5 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said **URL** link to said second application includes an encrypted address portion and said link to said web page provided by said first application includes a non-encrypted address portion" as in the present claimed invention. Levergood et al. describes a SID containing a 32-bit digital signature. However, as discussed above regarding claim 1, an SID is not equivalent to "URL address portion of said URL link" as in the present claimed invention. Therefore, Levergood et al. neither disclose nor suggest "said URL link to said second application includes an encrypted address portion and said link to said web page provided by said first application includes a non-encrypted address portion." Thus, Levergood et al. do not anticipate claim 5 of the present claimed invention.

CLAIM 7

Dependent claim 7 is considered to be patentable based on its dependence on claim 1. Claim 7 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion". Levergood et al. do not suggest such a feature combination for reasons given in connection with claim 1. The hash compression relied on in the Rejection of Levergood et al. column 5 lines 61-65 is of "items in the **SID** and the authorized **IP address**" and NOT of a "URL link address portion" as previously explained in connection with claim 1 (Levergood et al. column 5 lines 61-65, also see column 3 lines 33-37). Thus, Levergood et al. do not anticipate claim 7 of the present claimed invention.

CLAIM 8

Dependent claim 8 is considered to be patentable based on its dependence on claims 1 and 7. Claim 8 is also considered to be patentable because Levergood et al. neither disclose nor suggest that "said URL processor compresses said **URL link address portion** using a hash function". Levergood et al. merely states that the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers. This is not equivalent to "said URL processor compresses said **URL link address portion** using a hash function" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 8 of the present claimed invention.

CLAIM 9

Dependent claim 9 is considered to be patentable based on its dependence on claims 1 and 7. Claim 9 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said communication processor communicates said URL link address portion to a managing application for compression". Levergood et al. do not suggest such a feature combination for reasons given in connection with claim 1. Levergood et al. in column 5 lines 44-49 relied on in the Rejection merely mentions redirecting a URL to an authentication server for authenticating a **session identifier**. This has no bearing on communicating a "**URL link address portion** to a managing application for encryption" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 9 of the present claimed invention.

CLAIM 11

Independent claim 11 is considered to be patentable for the reasons given in connection with claim 1. In addition to features similar to claim 1, claim 11 describes "a

managing application for providing a common encryption key to a plurality of concurrently operating applications". This feature addresses the security deficiencies of prior art electronic systems, such as those described in Levergood et al. Specifically, as stated on page 11, lines 8-9 of the present specification, "In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted." The present invention as claimed in claim 11 accomplishes this goal.

Claim 11 is also considered to be patentable because Levergood et al. neither disclose nor suggest a feature combination including a "managing application for providing a **common encryption key** to a **plurality** of concurrently operating **applications**" as in the present claimed invention. Levergood et al. disclose an encryption key used for encrypting an IP address (NOT a URL address portion) is accessible by a content and authorization server (Levergood et al. column 5, lines 61-65) but fails to show or suggest an encryption key for encrypting a "URL address portion" is accessible from a "managing application for providing a **common encryption key** to a **plurality** of concurrently operating **applications**" as in the present claimed invention.

The claimed system addresses the security problem that is present in prior art system such as Levergood et al. by "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in the present claimed invention. However, the user selection of the embedded link to view laboratory test orders in browser command does not require the incorporation of the session identifier and other context

information, as stated on page 14, lines 34-36, "because the link to the test results page is an intra-application link there is no requirement for this particular embedded link to be processed in the manner previously described to incorporate the session identifier and other context information".

Levergood et al. neither disclose nor suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application" as in the present invention. Levergood et al. also fail to show or suggest doing this "by using said received encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link".

Applicant respectfully submits that the Rejection makes a **fundamental error** on page 4 in interpreting the Levergood et al. reference. Contrary to the Rejection statements on page 4, Levergood et al. in column 5 lines 61-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" on column 5, lines 61-65 (also see column 3, lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 11 of the present invention. The claimed "address portion" is NOT (and does NOT suggest) the "SID" or "IP Address" of Levergood et al.

Levergood et al. neither disclose nor suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL" as in the present claimed invention. Neither a session identifier nor an IP address as used in Levergood et al. are a "URL or a URL address portion" as in the present claimed invention. Indeed a URL and IP address are distinct and different objects with totally different functions. "The content server records the URL **and** the IP address" as stated in Levergood et al. in column 5, lines 37-38. An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" as described in column 2, lines 28-31 of Levergood et al. A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL as described on page 11, line 19 of the Specification.

Levergood et al. also neither disclose nor suggest the claim 11 feature combination involving "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application" as described in the present claimed invention. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" as described in column 3, lines 24-26 of Levergood et al. In contrast, the present claimed invention addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" as recited in page 11, lines 1-9, of the Specification.

Additionally, Levergood et al. neither disclose nor suggest the claim 11 feature of "including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application".

While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention. Consequently there is no reason, problem recognition or motivation for amending the Levergood et al. system to include the claimed arrangement. Withdrawal of the rejection of claim 11 under 35 USC 102(b) is respectfully requested.

CLAIM 12

Dependent claim 12 is considered to be patentable based on its dependence on claim 11. Claim 12 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said communication processor communicates said URL link address portion to a managing application for compression" as in the present claimed invention. Levergood et al. do not suggest a separate managing application used for compression of URL data and operating in conjunction with distinct "first and "second" applications. Levergood et al. in column 5 lines 44-49 relied on in the Rejection merely mentions redirecting a URL to an authentication server for authenticating a **session identifier**. Levergood et al. neither disclose nor suggest communicating the "URL link address portion to a managing application for compression" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 12 of the present claimed invention.

CLAIM 13

Dependent claim 13 is considered to be patentable based on its dependence on claim 11. Claim 13 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion" as in the present claimed invention. Levergood et al. do not suggest such a feature combination for reasons given in connection with claim 11.

The hash compression relied on in the Rejection of Levergood et al. column 5, lines 61-65 is of "items in the **SID** and the authorized **IP address**" and NOT of a "URL link address portion" as previously explained in connection with claim 11 (Levergood et al. column 5 lines 61-65, also see column 3 lines 33-37). Thus, Levergood et al. do not anticipate claim 13 of the present claimed invention.

CLAIM 14

Dependent claim 14 is considered to be patentable based on its dependence on claims 11 and 13. Claim 14 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said URL processor compresses said **URL link address portion** using a hash function" as in the present claimed invention. Levergood et al. merely states that the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers. Levergood et al. neither disclose nor suggest "said URL processor compresses said **URL link address portion** using a hash function" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 14 of the present claimed invention.

CLAIM 15

Dependent claim 15 is considered to be patentable based on its dependence on claims 11 and 13. Claim 15 is also considered to be patentable because Levergood et al. neither disclose nor suggest "said communication processor communicates said URL link address portion to a managing application for compression" as in the present claimed invention. Levergood et al. do not suggest such a feature combination for reasons given in connection with claim 11. Levergood et al. in column 5 lines 44-49 relied on in the Rejection merely mentions redirecting a URL to an authentication server for authenticating a **session identifier**. This has no bearing on communicating a "**URL link address portion**

to a managing application for encryption" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 15 of the present claimed invention.

CLAIM 18

Independent claim 18 recites a "system for processing URL link data for detecting unauthorized URL modification and suitable for use by a plurality of concurrently operating applications" comprising "a first application including, a URL processor for adaptively generating a URL link to a second application differently to a URL link to a web page provided by said first application, to provide a generated URL by using a received encryption key to encrypt a URL link address portion of said URL link to said second application and by non-encryption of said URL link to said web page provided by said first application; and a communication processor for including said generated URL in data representing a web page and for communicating said web page representative data including said generated URL to a requesting application". Claim 18 is considered to be patentable for the reasons given in connection with claim 1. Further, contrary to the Rejection statement on page 6, Levergood et al. in column 6, lines 17-26, neither disclose nor suggest incorporating "data representing a web page" of a URL generated by "using a received encryption key to encrypt a URL link address portion" as in the present claimed invention. Levergood et al. in column 6, lines 17-26 merely disclose search of a web page for links NOT incorporation of generated URL links in "data representing a web page" and specifically NOT incorporation in "data representing a web page" of a URL **generated by** "using a received encryption key to encrypt a **URL link address portion**" as in the present claimed invention. Thus, Levergood et al. do not anticipate claim 18 of the present claimed invention.

CLAIM 20

Independent claim 20 recites "A system supporting concurrent operation of a plurality of Internet compatible applications" comprising "a browser application including, a display generator for providing a user interface display permitting user entry of identification information and commands for a plurality of Internet compatible applications and for providing user identification information to a first application; a URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a non-encrypted session identifier; and a processor for initiating communication of said generated URL to said first application in response to validation of said user identification information, said first application having access to a key for decrypting said encrypted URL address portion". Claim 20 includes limitations similar to claim 1 discussed above and thus is considered to be patentable for reasons given in connection with claim 1.

CLAIM 21

Independent claim 21 describes a method employed by a first application for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. An encryption key is received and a URL link to a second application is processed differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link. The processed URL is included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application.

Contrary to the Rejection statements on page 3, Levergood et al. in column 5 lines 61-65 and column 3, lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" as described in column 5, lines 61-65 of Levergood et al. (also see column 3, lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 21 of the present invention. The claimed "address portion" is NOT (and does NOT suggest) the "SID" or "IP Address" of Levergood et al.

Levergood et al. neither disclose nor suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL" as in the present claimed invention. Neither a session identifier nor an IP address as used in Levergood et al. are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood et al. column 5, lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" as described in column 2, lines 28-31 of Levergood et al. A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL as described on page 11, line 19 of the Specification.

Levergood et al. also neither disclose nor suggest the claim 21 feature combination involving "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application" as in the present claimed invention. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3, lines 24-26). In contrast, the Specification addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" as described on page 11, lines 1-9.

Levergood et al. further neither disclose nor suggest the claim 21 feature of "for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application" as in the present claimed invention. While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention. Consequently there is no reason, problem recognition or motivation for amending the Levergood et al. system to include the claimed arrangement. Withdrawal of the rejection of claim 21 under 35 USC 102(b) is respectfully requested.

CLAIM 23

Independent claim 23 describes a method for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. A common encryption key is provided to the plurality of concurrently operating applications. An encryption key is received and a URL link to a second application is adaptively processed differently to an intra-application link to a web

page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link. The processed URL is included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application.

Contrary to the Rejection statements on page 3, Levergood et al. in column 5 lines 61-65 and column 3, lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" as described in column 5, lines 61-65 of Levergood et al. (also see column 3, lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 21 of the present invention. The claimed "address portion" is NOT (and does NOT suggest) the "SID" or "IP Address" of Levergood et al.

Levergood et al. neither disclose nor suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL" as in the present claimed invention. Neither a session identifier nor an IP address as used in Levergood et al. are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood et al. column 5, lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the

file, and the **path** to the file" as described in column 2, lines 28-31 of Levergood et al. A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL as described on page 11, line 19 of the Specification.

Levergood et al. also neither disclose nor suggest the claim 23 feature combination involving "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9).

Levergood et al. further neither disclose nor suggest the claim 23 feature of "for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention. Consequently there is no reason, problem recognition or motivation for amending the Levergood et al. system to include the claimed arrangement. Withdrawal of the rejection of claim 23 under 35 USC 102(b) is respectfully requested.

CLAIM 24

Independent claim 24 describes a method for processing URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. A URL link to a second application is adaptively generated differently to an intra-application URL link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to provide a generated URL. A key to the second application is provided for decrypting the encrypted URL address portion. The processed URL is included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application.

Contrary to the Rejection statements on page 3, Levergood et al. in column 5 lines 61-65 and column 3, lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" as described in column 5, lines 61-65 of Levergood et al. (also see column 3, lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 21 of the present invention. The claimed "address portion" is NOT (and does NOT suggest) the "SID" or "IP Address" of Levergood et al.

Levergood et al. neither disclose nor suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL" as in the present claimed invention. Neither a session identifier

nor an IP address as used in Levergood et al. are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood et al. column 5, lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" as described in column 2, lines 28-31 of Levergood et al. A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL as described on page 11, line 19 of the Specification.

Levergood et al. also neither disclose nor suggest the claim 24 feature combination involving "adaptively generating a URL link to a second application differently to an intra-application link to a web page provided by said first application". Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9).

Levergood et al. further neither disclose nor suggest the claim 24 feature of "for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention. Consequently there is no reason, problem recognition or motivation for amending the

Levergood et al. system to include the claimed arrangement. Withdrawal of the rejection of claim 24 under 35 USC 102(b) is respectfully requested.

In view of the above remarks, Applicant respectfully submits that there is no 35 USC 112 compliant enabling disclosure present in Levergood et al. that anticipates the present invention claimed in claims 1, 11, 18, 20, 21 and 23-24. As claims 2-9 are dependent on claim 1 and claims 12-15 are dependent on claim 11, Applicant respectfully submits that claims 2-9 and 12-15 are also not anticipated by Levergood et al. It is thus respectfully submitted that this rejection has been satisfied and should be withdrawn.

Rejection of Claims 10, 16, 17, 19 and 22 under 35 USC 103(a) over Levergood et al. (US Patent No. 5,708,780) in view of Berman et al. (US Patent No. 5,999,949).

Reversal of the rejection of claims 10, 16, 17, 19 and 22 under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. in view of Berman is respectfully requested. The rejection erroneously states that claims 10, 16, 17, 19 and 22 are obvious in view of Levergood et al. and further in view of Berman et al. for the reasons discussed herein below.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596, 1598 (Fed.Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art

references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion, or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. *Uniroya, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988); *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied,* 475 U.S. 1017 (1986); *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed.Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed.Cir. 1992).

CLAIM 10

Specifically, Berman et al. describes an automated networked service request and fulfillment system, including a client computer system in the offices of professionals such as doctor, and sponsor computers at the sites of service providers such as test labs or insurance companies. Service requests are prepared using a client system and automatically e-mailed to the sponsor system of an appropriate service provider. The request is fulfilled and the results are e-mailed back to the requesting client system using the mail server system.(See Berman et al., Abstract)

Dependent claim 10 is considered to be patentable based on its dependence on claim 1. Claim 10 is also considered to be patentable because Levergood et al. in view of Berman et al. neither disclose nor suggest "said URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application". Levergood et al. in view of Berman et al. does not suggest such a feature combination for reasons given in connection with claim 1. Specifically, in the

Berman et al. system messages are conveyed in SMTP (not HTTP protocol) format in accordance with the HL7 standard ("At the present time, e-mail messages sent over the Internet **must** be in standard SMTP format" - Berman et al. column 5 lines 61-62). Berman et al. does not even mention a URL. Contrary to the Rejection statement on page 7, there is no suggestion in Berman et al. (with Levergood et al.) in column 6 lines 2-15 or elsewhere of the claim 10 feature combination involving "adaptively" generating "URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application" together with an encrypted "**URL** link **address portion**" as in the present claimed invention.

Neither Levergood et al. nor Berman et al. recognize the advantages a "URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application" as in the present claimed invention. Levergood et al. and Berman et al. are concerned with different objectives and do not contemplate adaptively generating URL fields including encrypted patient specific information for incorporation in the URL link to a second application to accomplish the present claimed invention's support of multiple different concurrent Internet based application with the capability of conveying information between individual applications.

Further, combining the Levergood et al. system with the Berman et al. features as indicated by the Rejection results in a system for encrypting IP addresses and session identifiers for communication in email messages conveying patient specific information. Such a system does NOT show or suggest the claimed features. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID"

(Levergood et al. column 3 lines 24-26). The objective of Berman et al. is to provide an e-mail based system for making and fulfilling service requests between remote sites (Berman et al. column 2 lines 21-26) In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no common reason, problem recognition or motivation for combining the Levergood et al. and Berman et al. systems to provide the claimed arrangement. Consequently, withdrawal of the rejection of claim 10 under 35 USC 103(a) is respectfully requested.

CLAIM 16

Independent claim 16 recites a "system for encoding URL link data for use in detecting unauthorized URL modification" comprising "a browser application for providing a user interface display permitting user entry of identification information for providing user identification information to a first application; a first application responsive to said user identification information including, a URL processor for **adaptively generating URL fields** including an encrypted URL address portion and **encrypted patient specific information** for incorporation together with a non-encrypted portion in a processed URL; and a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". Claim 16 is considered to be patentable for the reasons given in connection with claims 1 and 10.

Neither Levergood et al. nor Berman et al. recognize the advantages a "URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application" as in the present claimed invention. Levergood et al. and Berman et al. are concerned with different

objectives and do not contemplate adaptively generating URL fields including encrypted patient specific information for incorporation in the URL link to a second application to accomplish the present claimed invention's support of multiple different concurrent Internet based application with the capability of conveying information between individual applications.

Further, combining the Levergood et al. system with the Berman et al. features as indicated by the Rejection results in a system for encrypting IP addresses and session identifiers for communication in email messages conveying patient specific information. Such a system does NOT show or suggest the claimed features. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). The objective of Berman et al. is to provide an e-mail based system for making and fulfilling service requests between remote sites (Berman et al. column 2 lines 21-26) In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no common reason, problem recognition or motivation for combining the Levergood et al. and Berman et al. systems to provide the claimed arrangement. Consequently, withdrawal of the rejection of claim 1 under 35 USC 103(a) is respectfully requested.

CLAIM 17

Dependent claim 17 is considered to be patentable based on its dependence on claim 16. Claim 17 is also considered to be patentable because Levergood et al. in view of Berman et al. neither disclose nor suggest "said communication processor communicates said URL address portion and said **encrypted patient specific information** to another

application for encryption". Levergood et al. (with Berman et al.) does not contemplate or mention encrypting a "URL address portion" and **"patient specific information"** within a URL at all.

Neither Levergood et al. nor Berman et al. recognize the advantages a "URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application" as in the present claimed invention. Levergood et al. and Berman et al. are concerned with different objectives and do not contemplate adaptively generating URL fields including encrypted patient specific information for incorporation in the URL link to a second application to accomplish the present claimed invention's support of multiple different concurrent Internet based application with the capability of conveying information between individual applications.

Further, combining the Levergood et al. system with the Berman et al. features as indicated by the Rejection results in a system for encrypting IP addresses and session identifiers for communication in email messages conveying patient specific information. Such a system does NOT show or suggest the claimed features. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). The objective of Berman et al. is to provide an e-mail based system for making and fulfilling service requests between remote sites (Berman et al. column 2 lines 21-26) In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no common reason, problem recognition or motivation for combining the Levergood et al. and Berman et al.

systems to provide the claimed arrangement. Consequently, withdrawal of the rejection of claim 17 under 35 USC 103(a) is respectfully requested.

CLAIM 19

Dependent claim 19 is considered to be patentable based on its dependence on claim 18. Levergood et al. in column 6, lines 17-26 neither disclose nor suggest incorporation in "data representing a web page" of a URL generated by "using a received encryption key to encrypt a URL link address portion" as in the present claimed invention. Levergood et al. in column 6 lines 17-26 merely disclose search of a web page for links NOT incorporation of generated URL links in "data representing a web page" and specifically NOT incorporation in "data representing a web page" of a URL **generated by** "using a received encryption key to encrypt a **URL link address portion**". Claim 19 is also considered to be patentable because Levergood et al. (with Berman et al.) does not show (or suggest) generation of "a URL field including **encrypted patient specific information** for incorporation in said generated URL link to said second application". Levergood et al. (with Berman et al.) does not convey encrypted data in a URL at all as explained in connection with claim 10.

CLAIM 22

Independent claim 22 describes a method employed by a first application for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications. An encryption key is received and a URL link to a second application is processed differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link. The processed URL is

included in data representing a web page and for communicating the web page representative data including the processed URL to a requesting application.

Contrary to the Rejection statements on page 9, Levergood et al. in column 5 lines 61-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood et al. state "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers"- Levergood et al. column 5 lines 61-65, also see column 3 lines 33-37). This is unlike the present claimed invention which uses "said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in claim 22 of the present invention. The claimed "address portion" is NOT (and does NOT suggest) the "SID" or "IP Address" of Levergood et al.

Levergood et al. do not show or suggest using a received "encryption key to encrypt a **URL** link **address portion** of said URL link to said second application to produce a processed URL". Neither a session identifier nor an IP address as used in Levergood et al. are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood et al. column 5 lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" (Levergood et al. column 2 lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11 line 19).

Levergood et al. also neither disclose nor suggest the claim 22 feature combination involving "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9).

Levergood et al. further neither disclose nor suggest the claim 22 feature of "for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". While Levergood et al. forward absolute URL links directed to controlled documents in different content servers, Levergood et al. neither disclose nor suggest "including said processed URL in data representing a web page" as in the present claimed invention. Consequently there is no reason, problem recognition or motivation for amending the Levergood et al. system to include the claimed arrangement.

Neither Levergood et al. nor Berman et al. recognize the advantages a "URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application." Neither Moore et al. nor Armga et al. contain any other problem recognition, reason or other motivation for incorporating the claimed feature arrangement. Levergood et al. and Berman et al. are concerned with different objectives and do not contemplate adaptively generating URL fields including encrypted patient specific information for incorporation in the URL link to

a second application to accomplish the Application's support of multiple different concurrent Internet based application with the capability of conveying information between individual applications. the Application scalability and form language adaptability advantages at all.

Further, combining the Levergood et al. system with the Berman et al. features as indicated by the Rejection results in a system for encrypting IP addresses and session identifiers for communication in email messages conveying patient specific information. Such a system does NOT show or suggest the claimed features. Further, the purpose of the Levergood et al. encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood et al. column 3 lines 24-26). The objective of Berman et al. is to provide an e-mail based system for making and fulfilling service requests between remote sites (Berman et al. column 2 lines 21-26) In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no common reason, problem recognition or motivation for combining the Levergood et al. and Berman et al. systems to provide the claimed arrangement. Consequently, withdrawal of the rejection of claim 22 under 35 USC 103(a) is respectfully requested.

Furthermore, Applicant respectfully submits that claim 10 is dependent on independent claim 1, and therefore the arguments presented above regarding claim 1 are applicable to dependent claim 10; claim 17 is dependent on independent claim 16, and therefore the arguments presented above regarding claim 16 are applicable to dependent claims 17; and claim 19 is dependent on independent claim 18, and therefore the arguments presented above regarding claim 18 are applicable to dependent claims 19.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure contained within either Levergood et al. or Berman et al., alone or in combination with one another, that makes the present invention as claimed in independent claims 1, 11, 16 and 18 unpatentable. As claims 10, 17, 19 and 22 are dependent on independent claims 1, 11, 16 and 18, it is respectfully submitted that claims 10, 17, 19 and 22 are also patentable. Therefore, it is further respectfully submitted that this rejection has been satisfied and should be withdrawn.

VIII CONCLUSION

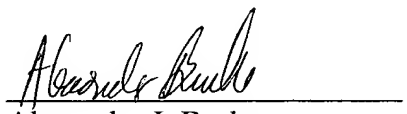
Levergood et al. do not show or suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Levergood et al. also fail to show or suggest doing this "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link".

Furthermore, neither Levergood et al. nor Berman et al., when taken alone or in any combination disclose or suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application".

Accordingly it is respectfully submitted that the rejection of Claims 1-24 should be reversed.

Respectfully submitted,
BARRY LYNN ROYER et al.

Date: September 6, 2005

By: 
Alexander J. Burke
Reg. No. 40,425

Siemens Corporation,
Customer No. 28524
Tel. 732 321 3023
Fax 732 321 3030

APPENDIX I - APPEALED CLAIMS

1. (Previously presented) A system employed by a first application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

an input processor for receiving an encryption key;

a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

2. (Previously presented) A system according to claim 1, wherein

said encryption key is accessible by said first and second applications from a managing application.

3. (Original) A system according to claim 1, wherein

said communication processor communicates said URL link address portion to a managing application for encryption.

4. (Previously presented) A system according to claim 1, wherein

said URL processor of said first application adaptively processes said URL link to said second application differently to said link to said web page provided by said first application in response to an identified URL type.

5. (Previously presented) A system according to claim 4, wherein

said URL link to said second application includes an encrypted address portion and said link to said web page provided by said first application includes a non-encrypted address portion.

6. (Original) A system according to claim 1, including

a browser application for providing a user interface display permitting user entry of identification information and for providing user identification information to said first application wherein

said first application authenticates said user identification information prior to permitting user access to functions of said first application.

7. (Original) A system according to claim 1, wherein

said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion.

8. (Original) A system according to claim 7, wherein

said URL processor compresses said URL link address portion using a hash function.

9. (Original) A system according to claim 7, wherein

said communication processor communicates said URL link address portion to a managing application for compression.

10. (Previously presented) A system according to claim 1, wherein

said URL processor adaptively generates URL fields including encrypted patient specific information for incorporation in said URL link to said second application.

11. (Previously presented) A system for encoding URL link data for use in detecting unauthorized URL modification occurring during concurrent operation of a plurality of applications, comprising:

a managing application for providing a common encryption key to a plurality of concurrently operating applications; and

a first application including,

an input processor for receiving said encryption key;

a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

12. (Original) A system according to claim 11, wherein

said communication processor communicates said URL link address portion to said managing application for encryption.

13. (Original) A system according to claim 11, wherein

said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion.

14. (Original) A system according to claim 13, wherein

said URL processor compresses said URL link address portion using a hash function.

15. (Original) A system according to claim 13, wherein

said communication processor communicates said URL link address portion to said managing application for compression.

16. (Previously presented) A system for encoding URL link data for use in detecting unauthorized URL modification, comprising:

a browser application for providing a user interface display permitting user entry of identification information for providing user identification information to a first application;

a first application responsive to said user identification information including,

a URL processor for adaptively generating URL fields including an encrypted URL address portion and encrypted patient specific information for incorporation together with a non-encrypted portion in a processed URL; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

17. (Previously presented) A system according to claim 16, wherein

said communication processor communicates said URL address portion and said encrypted patient specific information to another application for encryption.

18. (Previously presented) A system for processing URL link data for detecting unauthorized URL modification and suitable for use by a plurality of concurrently operating applications, comprising:

a first application including,

a URL processor for adaptively generating a URL link to a second application differently to a URL link to a web page provided by said first application, to provide a generated URL by using a received encryption key to encrypt a URL link address portion of said URL link to said second application and by non-encryption of said URL link to said web page provided by said first application; and

a communication processor for including said generated URL in data representing a web page and for communicating said web page representative data including said generated URL to a requesting application.

19. (Previously presented) A system according to claim 18, wherein

said URL processor, generates a URL field including encrypted patient specific information for incorporation in said generated URL link to said second application.

20. (Previously presented) A system supporting concurrent operation of a plurality of Internet compatible applications, comprising:

a browser application including,

a display generator for providing a user interface display permitting user entry of identification information and commands for a plurality of Internet compatible applications and for providing user identification information to a first application;

a URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a non-encrypted session identifier; and

a processor for initiating communication of said generated URL to said first application in response to validation of said user identification information, said first application having access to a key for decrypting said encrypted URL address portion.

21. (Previously presented) A method employed by a first application for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

receiving an encryption key;

processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and

including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

22. (Currently amended) A method employed by a first application operating in a system supporting concurrent operation of a plurality of Internet compatible applications, said method comprising the steps of:

in response to a command from a request device to initiate a first application,

enabling user operability of said first application based upon validation of user identification information;

forming a URL to provide a formed URL link by encrypting a link address to a second application and incorporating said encrypted link address, session identification information and encrypted patient specific information in said formed URL link;

including said formed URL link in data representing a web page to be returned to said request device; and

communicating to said request device, said web page representative data including said formed URL link.

23. (Previously presented) A method for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

providing a common encryption key to said plurality of concurrently operating applications; and

receiving said encryption key;

adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and

including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

24. (Previously presented) A method for processing URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

adaptively generating a URL link to a second application differently to an intra-application URL link to a web page provided by said first application by using a received

encryption key to encrypt a URL link address portion of said URL link to said second application to provide a generated URL;

providing a key to said second application for decrypting said encrypted URL address portion; and

including said generated URL in data representing a web page and for communicating said web page representative data including said generated URL to a requesting application.

APPENDIX II - EVIDENCE

Applicants rely on no evidence other than the arguments presented hereinabove.

APPENDIX III - RELATED PROCEEDINGS

Applicants respectfully submit that there are no related proceedings in this present application.

APPENDIX IV - TABLE OF CASES

1. *In re Fine*, 5 USPQ 2d 1600, (Fed Cir. 1988)
2. ACS Hospital Systems Inc v. Montefiore Hospital, 221 USPQ 929,933 (Fed. Cir. 1984)
3. *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966)
4. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988)
5. *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied,* 475 U.S. 1017 (1986)

APPENDIX V - LIST OF REFERENCES

U.S. Pat. No.	Issued Date	102(e) Date	Inventors
5,708,580	Jan 13, 1998		Levergood et al.

U.S. Pat. Pub. No.	Pub. Date	102(e) Date	Inventors
5,995,939	Nov. 30, 1999		Berman et al.

TABLE OF CONTENTS